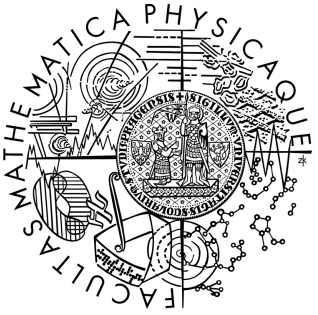
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Marcel Čurilla

Kořeny polynomů

Katedra Algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.,
Studijní program: Obecná matematika

2008

Ďakujem môjmu vedúcemu Liborovi Bartovi za vedenie tejto práce a prínosné konzultácie. Ďalej ďakujem Jánovi Bušovi z Technickej univerzity v Košiciach za pomoc pri písaní práce v TEXu. Mojím rodičom za podporu počas štúdia.

Prohlašuji, že jsem svou bakalářskou práci napsal(a) samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 29. května 2008 Marcel Čurilla

Obsah

Název práce: Kořeny polynomů
Autor: Marcel Čurilla
Katedra (ústav): Katedra Algebry
Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
e-mail vedoucího: libor.barto@gmail.com

Abstrakt: V predloženej práci pomocou Galoisovej teórie dokazujeme neexistenciu vzorca pre výpočet koreňov algebraickej rovnice stupňa väčšieho ako štyri. Galoisová teória nám umožnuje určité problémy v teórii telies previesť do teórie grúp, kde sa stávajú jednoduchšími. Budeme sa venovať normálnym, separabilným a radikálovým rozšíreniam telies. Definujeme Galoisovú grupu a ukážeme jej základné vlastnosti. Pomocou Základnej vety Galoisovej teórie prepojíme teóriu o telesách s teóriou grúp a ukážeme, ako súvisí riešiteľnosť rovnice s riešiteľnosťou jej Galoisovej grupy.

Klíčová slova: Galoisova teória, korene polynómov, riešiteľné grupy

Title: Roots of a polynomial
Author: Marcel Čurilla
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: libor.barto@gmail.com

Abstract: In this thesis we prove the non–existence of the formula for the computation of roots of polynomial equation with degree higher than four. We will do this by means of Galois theory, which allows us to reduce certain problems in the field theory to the group theory, where they become simpler. We will devote ourselves to the normal, separable and radical extension of the fields. We will define the Galois group and we will show its basic characteristics. Using the Fundamental theorem of the Galois theory, we will connect the fields theory with the gorup theory and we will show, how the solvability of the equation is related to the solvability of its Galois group.

Keywords: Galois theory, roots of a polynomial, solvable groups

1 Úvod

Cieľom tejto práce je dokázať neexistenciu vzorca na výpočet koreňov algebraickej rovnice stupňa väčšieho ako štvrtého. Algebraické rovnice majú bohatú históriu. Ich riešením sa zaoberali už starí Babylončania, ktorí už vtedy dokázali riešiť kvadratické rovnice. Vzorec na výpočet algebraickej rovnice tretieho stupňa bol prvykrát publikovaný až v roku 1545 talianským matematikom Girolamo Cardanom. O niekoľko rokov neskôr jeho žiak Lodovico Ferrari objavil vzorec na výpočet algebraickej rovnice štvrtého stupňa. Tieto vzorce sú známe ako Cardanove vzorce.

Matematici prirodzene očakávali, že ak existujú vzorce pre kvadratickú, kubickú a kvartickú rovnicu, musí takýto vzorec existovať aj pre rovnice vyšších stupňov. Ich metódy, ktoré boli použité na nájdenie vzorca pre kubické a kvartické, pre rovnicu piateho stupňa prestali fungovať. Takmer po 300 rokoch neúspešného hľadania vzorca, sa matematici začali zamýšľať, či takýto vzorec vôbec existuje.

V roku 1799 Paolo Ruffini publikoval 516 stránkový dôkaz neexistencie vzorca pre rovnice piateho stupňa, no dôkaz obsahoval veľa chýb a matematická spoločnosť o správnosti tohto dôkazu pochybovala. Otázka existencie (neexistencie) vzorca bola konečne vyriešená v roku 1824 Nielsom Henrikom Abelom. Dokázal, že neexistuje univerzálny vzorec pre algebraické rovnice piateho a vyššieho stupňa, v ktorom by sme z koeficientov a bežných algebraických operácií dostali korene rovnice. No pre niektoré rovnice piateho stupňa, ktoré majú špeciálny tvar, takýto vzorec existuje. Inak povedané, sú riešiteľné pomocou radikálov. Týmto vznikol nový problém, rozhodnúť, kedy je daná rovnica riešiteľná (neriešiteľná) pomocou radikálov a či náhodou nedokážeme riešiť každú rovnicu piateho stupňa pomocou iného vzorca.

Tento problém bol vyriešený v roku 1832 mladým francúzským matematikom Evariste Galoisom. Spôsob, ktorým tento problém dokázal bol na tú dobu prevratný. Galois spozoroval a dokázal vzťah medzi dvoma úplne odlišnými matematickými objektmi a ich vlastnosťami. Pomocou toho mohol určiť vlastnosť jedného objektu z vlastnosti toho druhého. Konkrétne, Galois priradil každej rovnici grupu, ktorú dnes nazývame Galoisovou grupou a dokázal, že algebraická rovnica je riešiteľná pomocou radikálov, práve keď táto grupa má určitú vlastnoť, dnes nazývanú riešiteľnosť.

Za zmienku určite stojí aj život tohto mladého a geniálneho matematika, ktorý dal základ Galoisovej teórie, ktorá je dnes jedným zo základných kameňov modernej algebry a zároveň niekoľkokrát neuspel v príjímacích pohovoroch na univerzitu. Bol revolucionárom za čo bol aj niekoľkokrát odsúdený. No väzení mal čas venovať sa matematike, kde vznikla aj väčšina jeho vedeckej

práce. Tie však v tej dobe neboli matematickou spoločnosťou prijaté. Uznanie dosiahli až v 70. rokoch minulého storočia. Galois zomrel ako 20 ročný v súboji o ženu. O jeho živote existuje množstvo biografickej literatúry, romány a dokonca sa jeho život stal predlohou k filmu. V tejto práci prevedieme dôkaz pomocou Galoisovej teórii.

V prvej kapitole „dokážeme“ neexistenciu univerzálneho vzorca na výpočet koreňov algebraickej rovnice stupňa väčšieho ako štvrtého. Dôkaz prevedieme podľa myšlienky Ruffiniho dôkazu, pričom sa zámerne dopustíme „chyby“, ktorej sa dopustil aj Ruffini. Tým získame výbornú motiváciu a pohľad do tohto problému. V druhej kapitole definujeme pojmy normálne a separabilné rozšírenie a ukážeme ich základné vlastnosti. Tretia kapitola je venovaná K-monomorfizmom telies. Zadefinujeme Galoisovú grupu telesa L, pozostávjúcu zo všetkých K-automorfizmov telesa L. V štvrtej kapitole ukážeme, že existuje bijektívne zobrazenie medzi podtelesami telesa L a podgrupami Galoisovej grupy telesa L. Piata kapitola je venovaná teórii grúp, kde ukážeme niektoré vlastnosti riešiteľných grúp. V šiestej kapitole definujeme radikálové rozšírenie a ukážeme ako súvisí radikálové rozšírenie s riešiteľnosťou Galoisovej grupy tohto rozšírenia. V poslednej kapitole nájdeme polynóm, ktorému je priradená neriešiteľná grupa, teda polynóm neriešiteľný pomocou radikálov.

2 Základné pojmy a značenie

V celom texte sa používa štandardné značenie. Teleso prirodzených, celých, racionálnych, reálnych a komplexných čisiel značíme $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$.

Podgrupu H grupy G značíme $H \leq G$. Grupu všetkých permutácií na množine $\{1, 2, \ldots, n\}$ značíme $\mathbb{S}_n$. Množina všetkých párnych permutácií z $\mathbb{S}_n$ je podgrupou grupy $\mathbb{S}_n$ a značíme ju $\mathbb{A}_n$. To, že N je normálna podgrupa grupy G budeme značiť $N \triangleleft G$. Nech $N \triangleleft G$, potom symbol G/N (resp. $\frac{G}{N}$) značí faktorgrupu grupy G podľa N.

Nech N je podteleso telesa L, čo značíme $N \leq L$, (L je rozšírenie N), potom teleso L je vektorový priestor nad N a môžeme definovať stupeň rozšírenia $N \leq L$, ako dimenziu vektorového priestoru L nad N, čo značíme $[L : N]$. Ak $[L : N] < \infty$ nazývame rozšírenie $N \leq L$ konečným rozšírením. Symbol $K[x]$ značí teleso polynómov nad telesom K jednej premennej x. Keďže v celej práci pracujeme s polynómami jednej premennej budeme pre jednoduchosť zapisovať: *polynóm f nad K* (resp. $f \in K[x]$).Rozšírenie telesa $K \leq L$ sa nazýva algebraické, ak pre každý prvok $\alpha \in L$ existuje nenulový polynóm $f \in K[x]$, že $f(\alpha) = 0$. Každé konečné rozšírenie je algebraické. Nech $K \leq L$ je algebraické rozšírenie a $\alpha \in L$, potom nenulový monický polynóm $m \in K[x]$ najmenšieho stupňa taký, že $m(\alpha) = 0$ nazývame minimálny polynóm prvku α nad K. Nech $K \leq L$, potom najmenšie teleso obsahujúce teleso K a prvok $\alpha \in L$ značime $K(\alpha)$. Ak $K \leq L$ je algebraické rozšírenie a $\alpha \in L$, potom $[K(\alpha) : K]$ je rovný stupňu minimálneho polynóm α nad K. Nech $K \leq M \leq L$ sú podtelesá $\mathbb{C}$, potom platí $[L : K] = [L : M][M : K]$.

Pre podgrupu G grupy $\mathrm{Aut}(L)$, grupy automorfizmov telesa L, definujeme $G^\dagger = \{\alpha,\ \alpha \in L;\ \forall\, \tau \in G$ platí $\tau(\alpha) = \alpha\}$. Platí $G^\dagger \leq L$. Ak platí $K \leq G^\dagger$, budeme hovoriť, že teleso K je grupou G fixované. Teleso $K = G^\dagger$ budeme nazývať maximálne teleso fixované grupou G.

3 Ruffiniho dôkaz

Cieľom tejto kapitoly je dôkaz vety o neexistencii spoločného vzorca pre výpočet koreňov polynómov nad $\mathbb{C}$ stupňa väčšieho ako päť.

My sa najprv pokúsime takýto vzorec nájsť a zistíme, prečo pre polynómy stupňa väčšieho ako päť, takýto vzorec neexistuje. Vzorcom budeme rozumieť výraz, ktorý dostaneme z koeficientov polynómu a konečného počtu operácií $\{\sqrt[n]{\cdot}, +, -, /, \cdot\}$. Nech $F(t)$ je ľubovoľný polynóm stupňa n nad $\mathbb{C}$, ktorého korene sú $t_1, \ldots, t_n \in \mathbb{C}$. Teda $F(t) = (t - t_1) \ldots (t - t_n)$ a po roznásobení dostávame

$$F(t) = t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n, \tag{3.1}$$

kde s_j sú elementárne symetrické polynómy

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n \\ s_2 &= t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n \\ &\vdots \\ s_n &= t_1 \cdots t_n. \end{aligned}$$

Uvažujme teleso $K = \mathbb{C}(s_1, \ldots, s_n)$, čo značí teleso racionálnych funkcií nezávislých komplexných premenných $s_1, \ldots, s_n$ nad $\mathbb{C}$. Jedná sa o množinu všetkých výrazov, ktoré dostaneme z $s_1, \ldots, s_n$ a operácií $\{+, -, /, \cdot\}$. My sa pokúsime vytvoriť nadteleso L telesa K, ktoré budeme konštruovať z telesa K postupným pridávaním odmocnín, pokiaľ nedostaneme teleso, v ktorom už vyjadriť korene polynomu dokážeme. A tým aj každú racionálnu funkciu premenných $t_1, \ldots, t_n$, sme schopní zapísať pomocou $s_1, \ldots, s_n$ a konečného počtu operácií $\{\sqrt[n]{\cdot}, -, +, /, \cdot\}$. Teleso racionálnych funkcií premenných $t_1, \ldots, t_n$ budeme značiť $L = \mathbb{C}(t_1, \ldots, t_n)$. Ako príklad si uveďme ako by sme postupovali pri riešení algebraickej rovnici druhého stupňa.

Príklad 3.1. Nech $F(t) = (t - t_1)(t - t_2) = t^2 - s_1 t + s_2 = 0$. Rozšírime teleso $\mathbb{C}(s_1, s_2)$ o odmocninu $\sqrt{{s_1}^2 - 4s_2}$, t. j.

$$\mathbb{C}(s_1, s_2) \leq \mathbb{C}(s_1, s_2)(\sqrt{{s_1}^2 - 4s_2}) = P,$$

v tomto telese P sme už schopní vyjadriť korene ako

$$t_1 = \frac{s_1 + \sqrt{{s_1}^2 - 4s_2}}{2} \quad \text{a} \quad t_2 = \frac{s_1 - \sqrt{{s_1}^2 - 4s_2}}{2},$$

a teda aj každú racionálnu funkciu z $\mathbb{C}(t_1, t_2)$, sme schopní vyjadriť pomocou s_1, s_2 a operácií $\{\sqrt[n]{\cdot}, +, -, /, \cdot\}$. Preto $P = \mathbb{C}(t_1, t_2)$.

Prvok grupy permutácií $\sigma \in \mathbb{S}_n$ pôsobí na prvok $f \in L$ nasledovne

$$\sigma f(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).$$

Prvok $f \in L$, pre ktorý platí $\sigma(f) = f$ pre $\forall \sigma \in \mathbb{S}_n$, nazývame symetrická racionálna funkcia. Teleso K pozostávajúce zo všetkých symetrických racionálnych funkcií z telesa $L = \mathbb{C}(t_1, \ldots, t_n)$, je generované n elementárnymi symetrickými polynómami. Teda $K = \mathbb{C}(s_1, \ldots, s_n)$. Dôkaz tohto tvrdenia nájdeme napríklad v [4].

Príklad 3.2. Nech $L = \mathbb{C}(t_1, t_2, t_3)$, $f, g \in L$ a $\sigma = (12) \in \mathbb{S}_3$. Potom

$$f = \frac{t_1 + t_2 t_3 - t_1^3 t_3^2}{t_1 t_2 + t_1 t_3 + t_2 t_3} \qquad \text{a} \qquad g = \frac{t_1^2 + t_2^2 + t_3^2}{t_1 t_2 t_3}$$

$$\sigma(f) = \frac{t_2 + t_1 t_3 - t_2^3 t_3^2}{t_2 t_1 + t_2 t_3 + t_1 t_3} \qquad \text{a} \qquad \sigma(g) = \frac{t_2^2 + t_1^2 + t_3^2}{t_2 t_1 t_3} = g.$$

Je vidieť, že $\sigma(g)$ sa rovná g a $g(t_1, t_2, t_3)$ je symetrická racionálna funkcia, t. j. $g \in K$. To znamená, že g sa dá zapísať ako lineárna kombinácia s_1, s_2, s_3. A naozaj $g = (s_1^2 - s_2)/s_3$, teda $g \in K$.

Teraz sa pokúsime tieto úvodné úvahy sformalizovať. Nasledujúca definícia nie je štandardná, no jej pomenovanie je opodstatnené, pretože odráža predpoklady a úvahy, ktoré Ruffini urobil pri jeho dôkaze neexistencie vzorca pre rovnice piateho stupňa.

Definícia 3.3. *Algebraická rovnica $F(t) = 0$ z (3.1) je riešiteľná pomocou Ruffiniho radikálov, ak existuje konečná postupnosť podtelies*

$$\mathbb{C}(s_1, \ldots, s_n) = K = K_0 \leq K_1 \leq \cdots \leq K_r = L = \mathbb{C}(t_1, \ldots, t_n) \tag{3.2}$$

takých, že pre $j = 0, \ldots, r-1$ je

$$K_{j+1} = K_j(\alpha_j) \;\; a \;\; {\alpha_j}^{n_j} \in K_j \;\; pre \;\; n_j \in \mathbb{N}.$$

V definícií 3.3 teleso K racionálnych funkcií premenných $s_1, \ldots, s_n$, t. j. koeficientov polynómu (3.1), rozširujeme postupne pomocou odmocnín. Ak máme konečnú postupnosť (3.2), tak sme schopní každú racionálnu funkciu premenných $t_1, \ldots, t_n$, teda aj funkcie t_j, vyjadriť pomocou premenných $s_1, \ldots, s_n$ a konečného počtu operácií $\{\sqrt[n]{\cdot}, +, -, /, \cdot\}$. To nám dáva existenciu spoločného vzorec na výpočet koreňov $t_1, \ldots, t_n$ ľubovoľnej algebraickej rovnice nad komplexnými číslami.

Ruffini vo svojom dôkaze mlčky predpokladal, že ak polynóm $F(t)$ je riešiteľný pomocou radikálov, tak sú tieto radikály vyjadrené ako racionálne funkcie jeho koreňov. No nie je tažké predstaviť si, že riešenie pomocou radikálov môže existovať, no α_j skonštruované týmto spôsobom, by mohli ležať až v nejakom rozšírení telesa L. (Napríklad riešenie rovnice $t^5 - s_1 = 0$.) Až Abel dokázal, že *ak polynomiálna rovnica $F(t) = 0$ je riešiteľná pomocou radikálov, potom sú tieto radikály vyjadrené ako racionálne funkcie jeho koreňov* – je riešiteľná pomocou Ruffiniho radikálov. Čím odstránil hlavný nedostatok (chybu) z Ruffiniho dôkazu. Dôkaz tejto Abelovej vety je hlavným problémom v dôkaze neexistencie vzorca pre korene polynómov stupňa väčšieho než štvrtého. My tento problém obídeme pomocou definície 3.3 a ako kompenzáciu získame výbornú motiváciu a pohľad do tohto problému a porozumieme tomu, akú rolu v dôkaze hrajú permutácie.

Tvrdenie 3.4. *Konečnú postupnosť z definície 3.3 môžeme upraviť (predĺžiť) tak, aby všetky n_j boli prvočísla.*

Dôkaz. Pre fixné j vezmime dvojicu telies z (1.2) $K_j \leq K_{j+1} = K_j(\alpha)$, teda $\alpha^{n_j} = \alpha^{p_1 p_2 \cdots p_n} \in K$. Potom toto rozšírenie môžeme skonštruovať vložením medzitelies medzi K_j a K_{j+1}:

$$K_j \leq K(\alpha^{p_1 p_2 \cdots p_{n-1}}) \leq \cdots \leq K(\alpha^{p_1}) \leq K(\alpha) = K_{j+1},$$

kde $(\alpha^{p_1 p_2 \cdots p_l})^{p_{l+1}} \in K(\alpha^{p_1 p_2 \cdots p_{l+1}})$ a $l \in \{0 \ldots n-1\}$. □

V nasledujúcej vete budú použité neskôr dokázané lemy 7.12 a 7.11 v kapitole 7, ktorú je možné čítať samostatne.

Veta 3.5. *Algebraická rovnica $F(t) = 0$ stupňa n nie je riešiteľná pomocou Ruffiniho radikálov pre $n \geqq 5$.*

Dôkaz. Nech $F(t)$ je riešiteľná pomocou Ruffiniho radikálov a $n \geqq 5$. Potom existuje postupnosť podtelies (3.3), kde $n_j = p_j$ sú prvočísla a

$$K \leq K_1 \leq \cdots \leq L,$$

kde $K_1 = K(\alpha_1)$, ${\alpha_1}^{p_1} \in K$ a $\alpha_1 \notin K$. Teleso K je fixované grupou $\mathbb{S}_n$. To znamená ak $\sigma \in \mathbb{S}_n$ a $x \in K$, potom $\sigma(x) = x$. Nech $p_1 = p$

$$(\sigma(\alpha_1))^p = (\sigma({\alpha_1}^p)) = {\alpha_1}^p$$

Z toho plynie, že $\sigma(\alpha_1) = \zeta^{j(\sigma)}\alpha_1$, kde ζ je p-tá odmocnina z jednotky a $j(\sigma) = 0, \ldots, p-1$. Keďže platí $\zeta^a\zeta^b = \zeta^{(a+b) \bmod p}$, množina všetkých p-tých

odmocnín z jednotky v $\mathbb{C}$ je multiplikatívna grupa, cyklická a izomorfná grupe $\mathbb{Z}_p$. Uvažujme zobrazenie

$$\begin{aligned} \psi : \mathbb{S}_n &\rightarrow \mathbb{Z}_p \\ \psi(\sigma) &= j(\sigma). \end{aligned}$$

Zobrazenie ψ je zrejme grupový homomorfizmus. Keďže $\alpha_1 \notin K$ musí byť zobrazenie ψ netriviálne. A z dôvodu, že $\mathbb{Z}_p$ nemá netriviálnu podgrupu je ψ aj surjektívne. Z vety o izomorfizme dostávame, že $\mathbb{S}_n/\mathrm{Ker}(\psi) \cong \mathbb{Z}_p$. Teda $\mathrm{Ker}(\psi)$ je netriviálna normálna podrupa grupy $\mathbb{S}_n$. Z dôsledku 7.11 vyplýva, že $\mathrm{Ker}(\psi) = \mathbb{A}_n$. To znamená, že α_1 je fixovaná grupou $\mathbb{A}_n$. A teda všetky prvky z K_1 sú fixované $\mathbb{A}_n$.

V ďalšom kroku nájdeme najväčšie $m \in \mathbb{N}$ také, že

$$\underbrace{K \leq K_1 \leq \cdots \leq K_m}_{\text{fixovane } \mathbb{A}_n} \leq \cdots \leq L$$

Pritom teleso K_{m+1} už nie je fixované $\mathbb{A}_n$ a

$$K_{m+1} = K_m(\alpha_m)\,, {\alpha_m}^{p_m} \in K_m\,, \alpha_m \notin K_m.$$

Rovnako ako v predchádzajúcom prípade nám α_m definuje grupový homomorfizmus $\psi : \mathbb{A}_n \rightarrow \mathbb{Z}_p$, pričom opäť je $\mathrm{Ker}(\psi)$ netriviálna normálna podgrupa grupy $\mathbb{A}_n$, čo je spor s dôsledkom 7.12. □

Vo vete 3.5 sme dokázali, že všeobecná algebraická rovnica stupňa n nie je riešiteľná pomocou Ruffiniho radikálov pre $n \geqq 5$ a podľa vyššie vyslovenej vety od Abela, ktorej dôkaz neuvádzame, nie je rovnica $F(t) = 0$ riešiteľná pomocou radikálov.

A prečo nie sme s prácou hotoví? My sme dokázali to, že pre algebraické rovnice stupňa $n \geqq 5$ neexistuje univerzálny vzorec na výpočet koreňov tejto rovnice. My ale môžeme byť schopní riešiť algebraickú rovnicu stupňa $n \geqq 5$ pomocou radikálov, použitím iného vzorca pre každý polynóm. Dokonca by sme mohli byť schopní rozdeliť rovnice piateho stupňa na niekoľko typov a pre každý typ rovníc nájsť vzorec na výpočet koreňov.

Na to, že to nie je možné prišiel mladý francúzsky matematik Evariste Galois, ktorý každému polynómu jednoznačne priradil grupu. A dokázal, že polynóm je riešiteľný pomocou radikálov, práve keď jeho grupa má určitú vlastnosť (je riešiteľná). To nám dáva nutnú a postačujúcu podmienku na určenie, kedy je polynóm riešiteľný (neriešiteľný) pomocou radikálov. Nám ostáva už len nájsť grupu, ktorá túto vlastnosť nebude mať a nájsť polynóm, ktorému je táto grupa priradená.

Veta 3.5 nám síce nehovorí nič o existencii vzorca pre algebraické rovnice stupňa menšieho než päť, ale z jej dôkazu sa dá vyčítať, ako by sme mali postupovať pri hľadaní vzorca na výpočet jej koreňov.

Príklad 3.6. Podľa dôkazu vety 3.5 ilustrujme riešenie polynomiálnej rovnice tretieho stupňa. Prvé, čo potrebujeme urobiť je rozšíriť teleso $K = \mathbb{C}(s_1, s_2, s_3)$, o odmocninu z tohto telesa, tak aby teleso K bolo fixované grupou $\mathbb{A}_3$ ($K \leq {\mathbb{A}_3}^\dagger$).

Nech $K \leq K(\alpha)$ kde $\alpha = (t_1 - t_2)(t_1 - t_3)(t_2 - t_3)$. Je vidieť, že $\alpha^2 \in K$. My budeme potrebovať dokázať viac, ak h je fixované $\mathbb{A}_3$, potom $h \in K(\alpha)$. Ľubovoľná permutácia z $\mathbb{S}_3$ zobrazí $\alpha \to \pm\alpha$. (Párna permutácia z $\mathbb{A}_3$ prvok α fixuje a nepárna zobrazuje na $-\alpha$.)

Nech teda $h \in L$ je fixované $\mathbb{A}_3$ a nech $\tau = (12) \in \mathbb{S}_3 \backslash \mathbb{A}_3$ zapíšme $h = h^e + h^o$ kde

$$h^e = \frac{1}{2}(h + \tau(h)) \text{ a } h^o = \frac{1}{2}(h - \tau(h)).$$

Teda h^e je fixované $\mathbb{A}_3$ a takisto je fixované permutáciou τ. Keďže $\mathbb{S}_3$ je generovaná $\mathbb{A}_3$ a τ, patrí prvok h^e do K. Podobne h^o je fixované $\mathbb{A}_3$ a $\tau(h^o) = -h^o$. Potom prvok αh^o je fixovaný $\mathbb{S}_3$, teda $\alpha h^o \in K$ odkiaľ $h^o \in K(\alpha)$. A preto, $h = h^e + h^o \in K \cup K(\alpha) = K(\alpha)$. Dokázali sme, že $K = {\mathbb{A}_3}^\dagger$.

Nakoniec potrebujeme rozšíriť teleso $K(\alpha)$ o odmocninu z tohto telesa, aby sme dostali teleso $\mathbb{C}(t_1, t_2, t_3)$. Rozšírime ho o prvky y, z, kde

$$y = t_1 + \omega t_2 + \omega^2 t_3 \text{ a } z = t_1 + \omega t_3 + \omega^2 t_2,$$

pričom $1 \neq \omega^3 = 1$. Počítaním dokážeme, že y^3, z^3 sú fixované $\mathbb{A}_3$. Podľa vyššie dokázaného je $y^3, z^3 \in K(\alpha)$. Pritom $y^3 + z^3$ a $y^3 z^3$ sú fixované $\mathbb{S}_3$ (nepárna permutácia vymení y^3 s z^3), teda patria do K. To znamená, že že y^3, z^3 sú korene kvadratického polynómu $x^2 - (y^3 + z^3)x + y^3 z^3$, čo je polynóm s koeficientami v K a na výpočet koreňov z koeficientov algebraickej rovnice druhého stupňa máme vzorec. Teda y a z sú odmocniny z výrazu zloženého z koeficientov.

$$\begin{aligned} t_1 &= \frac{1}{3}(s_1 + y + z) \\ t_2 &= \frac{1}{3}(s_1 + \omega^2 y + \omega z) \\ t_3 &= \frac{1}{3}(s_1 + \omega y + \omega^2 z). \end{aligned}$$

Teleso $K(\alpha, y, z) = \mathbb{C}(t_1, t_2, t_3)$, pričom $\alpha^2 \in K$, $y^3 \in K(\alpha)$ a $z^3 \in K(\alpha, y^3)$ a $\mathbb{S}_3/\mathbb{A}_3 \cong \mathbb{Z}_2$ a $\mathbb{A}_3/1 \cong \mathbb{Z}_3$. Z toho vyplýva, že algebraická rovnica tretieho stupňa je riešiteľná pomocou Ruffiniho radikálov.

4 Normálne a separabilné rozšírenie

V tejto kapitole zadefinujeme pojmy normálne a separabilné rozšírenie a ukážeme ich základné vlastnosti.

Niektoré tvrdenia sú uvedené bez dôkazu, ktorý nájdete napríklad v [4].

Definícia 4.1. *Nech K je teleso a polynóm $f \in K[x]$ stupňa n. Teleso U sa nazýva rozkladovým nadtelesom polynómu f, ak $K \leq U$ a platí:*

1. *Polynóm f sa v U rozkladá na lineárne činitele.*
2. *Ak $K \leq \tilde{U} \leq U$ a f sa v $\tilde{U}$ rozkladá na lineárne činitele, tak $\tilde{U} = U$.*

Druhá podmienka je ekvivalentná rovnosti $U = K(a_1, \ldots, a_n)$, kde a_i sú korene polynómu f v U.

Tvrdenie 4.2. *Pre každý polynóm nad $K \leq \mathbb{C}$ existuje rozkladové nadteleso U a stupeň tohto rozšírenia je konečný.*

Príklad 4.3. Nech $f(x) = (x^2 - 3)(x^3 + 1)$ je polynóm nad $\mathbb{Q}$. Rozkladové nadteleso polynómu f môžeme skonštruovať nasledujúcim spôsobom. Polynóm f sa v $\mathbb{C}$ rozkladá na lineárne činitele

$$f(t) = (t + \sqrt{3})(t - \sqrt{3})(t + 1)\left(t - \frac{1 + i\sqrt{3}}{2}\right)\left(t - \frac{1 - i\sqrt{3}}{2}\right),$$

takže rozkladové nadteleso je $U = \mathbb{Q}\left(\sqrt{3}, \frac{1+i\sqrt{3}}{2}\right) = \mathbb{Q}(\sqrt{3}, i)$.

Definícia 4.4. *Rozšírenie telesa $K \leq L$ sa nazýva normálne, ak pre každý ireducibilný polynóm $f \in K[x]$, ktorý má koreň v L, je teleso L jeho rozkladovým nadtelesom.*

Príklad 4.5. $\mathbb{R} \leq \mathbb{C}$ je normálnym rozšírením telesa $\mathbb{R}$, pretože každý polynóm nad $\mathbb{R}$ sa v $\mathbb{C}$ rozkladá. Príklad na rozšírenie, ktoré nie je normálne, je $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$. Ireducibilný polynóm $x^3 - 2$ má koreň v $\mathbb{Q}(\sqrt[3]{2})$, no toto teleso nie je jeho rozkladovým nadtelesom.

Veta 4.6. *Rozšírenie telies $K \leq L$ je normálne a konečné, práve keď existuje polynóm f nad K taký, že teleso L je jeho rozkladovým nadtelesom.*

Definícia 4.7. *Nech L je konečné rozšírenie telesa K. Normálny uzáver tohto rozšírenia je teleso N také, že $L \leq N$ a platí:*

1. *$K \leq N$ je normálne.*
2. *Ak $L \leq \tilde{N} \leq N$ a $K \leq \tilde{N}$ je normálne, potom $\tilde{N} = N$.*

Tvrdenie 4.8. *Ak $K \leq L$ je konečné rozšírenie v $\mathbb{C}$, potom existuje jediný normálny uzáver tohto rozšírenia, ktorý je konečným rozšírením K.*

Príklad 4.9. Nech $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$. Z príkladu 4.5 vieme, že toto rozšírenie nie je normálne. Položme $N = \mathbb{Q}(c, cw, cw^2) = \mathbb{Q}(c, w)$ kde $c = \sqrt[3]{2}$ a w je komplexný koreň $\sqrt[3]{1}$, $w = (-1 + i\sqrt{3})/2$. Teda N sme dostali pridaním všetkých chýbajúcich koreňov.

Definícia 4.10. *Nech $K \leq L$, potom ireducibilný polynóm f nad telesom K sa nazýva separabilný v L, práve keď polynóm f má v S len jednoduché korene.*

Definícia 4.11. *Algebraické rozšírenie $K \leq L$ sa nazýva separabilné, ak pre každé $\alpha \in L$ je minimálny polynóm prvku α nad K separabilný.*

Lema 4.12. *Ak K je podteleso $\mathbb{C}$, tak platí, že každý ireducibilný polynóm je v $\mathbb{C}$ separabilný.*

Dôkaz. Nech $f \in K[x]$ je ireducibilný a nech nie je separabilný (má viacnásobné korene), teda f a $D(f)$, kde D je operátor derivovania, majú spoločného deliteľa g stupňa väčšieho než jedna. Keďže f je ireducibilný, musí byť $g = f$ a pretože $\deg(D(f)) \leq \deg(f)$, musí byť $D(f) = 0$, čo implikuje, že f je konštantný polynóm. □

Myšlienku normálneho rozšírenia priniesol Galois a pretože pracoval nad komplexnými číslami separabilné rozšírenie dostal automaticky.

5 Monomorfizmus telies

V tejto kapitole si vybudujeme teóriu potrebnú pre dôkaz Základnej vety Galoisovej teórie.

Zadefinujeme si Galoisovu grupu konečného rozšírenia a pozrieme sa, ako súvisí s týmto rozšírením. Uvedieme ekvivalentné podmienky normálneho rozšírenia. V celej kapitole budeme pracovať s telesami v $\mathbb{C}$, čo vo väčšine prípadov znamená vynechanie predpokladu separability.

Lema 5.1 (Dedekind)**.** *Nech K je podteleso telesa L, potom každá množina rôznych monomorfizmov (prostých homomorfizmov) z K do L je lineárne nezávislá nad L.*

Dôkaz. Nech $\lambda_1, \ldots, \lambda_n$ sú rôzne monomorfizmy $K \to L$. Tieto monomorfizmy sú lineárne nezávislé nad L práve vtedy, ak je rovnosť

$$a_1\lambda_1(x) + \cdots + a_n\lambda_n(x) = 0 \quad \text{kde } a_i \in L, \qquad \forall x \in K \tag{5.1}$$

splnená jedine ak $a_i = 0$ pre $i = 1 \ldots n$.

Vetu dokážeme matematickou indukciou vzhľadom k n, t. j. k počtu rôznych monomorfizmov. Nech $n = 1$. Ak by platilo, že $a_1\lambda_1(x) = 0$, kde $a_1 \neq 0$. Potom vyplýva $\lambda_1(x) = 0$ pre $\forall x \in K$, čo je spor s tvrdením, že λ_1 je monomorfizmus.

Urobíme indukčný predpoklad. Budeme predpokladať, že rovnica $a_1\lambda_1 + + \cdots + a_k\lambda_k = 0$ pre $k < n$ má len triviálne riešenie.

Predpokladajme, že rovnica (5.1) má netriviálne riešenie. Ak by nejaké $a_i = 0$ potom z indukčného predpokladu dostávame, že $a_i = 0$ pre všetky i, teda $a_i \neq 0$ pre $\forall i \in 1 \ldots k$. Z $\lambda_1 \neq \lambda_n$ vyplýva existencia $y \in K$, že $\lambda_1(y) \neq \lambda_n(y)$ Dosadením prvku $xy \in K$ do rovnice (5.1) dostávame:

$$\begin{aligned} a_1\lambda_1(xy) + \cdots + a_n\lambda_n(xy) &= 0 \\ a_1\lambda_1(x)\lambda_1(y) + \cdots + a_n\lambda_n(x)\lambda_n(y) &= 0 \end{aligned}$$

Vynásobením rovnice (5.1) prvkom $\lambda_n(y)$ dostávame:

$$a_1\lambda_1(x)\lambda_n(y) + \cdots + a_n\lambda_n(x)\lambda_n(y) = 0$$

Odčítaním týchto rovníc dostávame rovnosť

$$\left[a_1\left(\lambda_1(y) - \lambda_n(y)\right)\right]\lambda_1(x) + \cdots + \left[a_{n-1}\left(\lambda_{n-1}(y) - \lambda_n(y)\right)\right]\lambda_{n-1}(x) = 0$$

kde $a_1\left(\lambda_1(y) - \lambda_n(y)\right) \neq 0$, čo je spor s indukčným predpokladom. □

Veta 5.2. *Nech G je konečná podgrupa grupy automorfizmov telesa K a nech $K_0 = G^\dagger$. Potom $[K : K_0] = |G|$.*

Dôkaz. Množina všetkých automorfizmov telesa K, vzhľadom k operácií skladania zobrazení, je grupa a nazývame ju grupou automorfizmov telesa K.

Nech $|G| = n$ t. j. $G = \{g_1, g_2, \ldots, g_n\}$, kde $g_1 = 1$, čo je identické zobrazenie.

1. Predpokladajme $[K : K_0] = m < n$.
Nech $\{x_1, \ldots, x_m\}$ je báza vektorového priestoru K nad K_0. Potom sústava rovníc s neznámymi $y_1, \ldots, y_n \in K$

$$\begin{aligned} y_1 g_1(x_1) + \cdots + y_n g_n(x_1) &= 0 \\ &\vdots \\ y_1 g_1(x_m) + \cdots + y_n g_n(x_m) &= 0 \end{aligned}$$

má m riadkov a $n > m$ neznámych, teda má netriviálne riešenie. Ľubovoľný prvok $x \in K$ sa dá vyjadriť ako $x = \alpha_1 x_1 + \cdots + \alpha_1 x_m$, kde $\alpha_i \in K_0$. Po úprave využijúc vlastnosti linearity automorfizmov, dostávame rovnost: $y_1 g_1(x) + \cdots + y_n g_n(x) = 0$ pre $\forall x \in K$. A pretože $g_1, \ldots, g_n$ sú rôzne a teda lineárne nezávislé automorfizmy nad K, podľa predchádzajúcej lemy dostávame spor.

2. Predpokladajme $[K : K_0] > n$.
Potom existuje množina prvkov $\{x_1, \ldots, x_{n+1}\}$ kde $x_i \in K$, ktorá je lineárne nezávislá. Sústava rovníc s neznámymi $y_1, \ldots, y_{n+1} \in K$

$$y_1 g_j(x_1) + \ldots + y_{n+1} g_j(x_{n+1}) = 0, \text{ kde} \quad j = 1 \ldots n \tag{5.2}$$

má netriviálne riešenie. Netriviálne riešenie $y_1, \ldots, y_{n+1}$ sústavy 5.2 vyberieme tak, aby ich bolo čo najviac nulových.

$$y_1, \ldots, y_r \neq 0\,, \quad y_{r+1}, \ldots, y_{n+1} = 0$$

Takže predošlú sústavu rovníc (5.2) môžeme prepísať na

$$y_1 g_j(x_1) + \cdots + y_r g_j(x_r) = 0, \quad j = 1 \ldots n \tag{5.3}$$

Nech $g \in G$ a použime g na rovnosť (5.3). Po úprave dostávame sústavu rovníc

$$g(y_1)g(g_j(x_1)) + \cdots + g(y_r)g(g_j(x_r)) = 0, \quad j = 1, \ldots, n.$$

Pretože zobrazenie $g_i \to g g_i$ je bijekcia $G \to G$. Môžeme predošlú sústavu

rovníc prepísať na

$$g(y_1)g_j(x_1) + \cdots + g(y_r)g_j(x_r) = 0, \quad j = 1, \ldots, n \tag{5.4}$$

Vynásobením rovnice (5.3) číslom $g(y_1)$ a rovnice (5.4) číslom y_1 a ich vzájomným odčítaním dostávame

$$[y_2 g(y_1) - g(y_2)y_1]\, g_j(x_2) + \cdots + [y_r g(y_1) - g(y_r)y_1]\, g_j(x_r) = 0, \quad j = 1, \ldots, n.$$

Aby sme neobdržali spor s voľbou r, musí byť $y_i g(y_1) - g(y_i)y_1 = 0$. To znamená, že

$$g(y_i {y_1}^{-1}) = y_i {y_1}^{-1} \quad \text{pre } \forall g \in G$$

teda $y_i {y_1}^{-1} \in K_0$. Teda existujú $z_1, \ldots, z_r \in K_0$ a $k \in K$ také, že $y_i = kz_i$ pre $i \in 1, \ldots, r$. Rovnica (5.3) pre $j = 1$ je

$$x_1 k z_1 + \cdots x_r k z_r = 0 \quad \text{predpokladáme, že } g_1 \text{ je identita}$$

a keďže $k \neq 0$ dostávame po vydelení k spor s predpokladom, že x_i sú lineárne nezávislé nad K_0.

Teda $n \leq [K : K_0] \leq n$, z čoho vyplýva $[K : K_0] = n$. □

Definícia 5.3. *Nech $K \leq M \leq L$ sú telesá, potom K-monomorfizmus telesa M do L nazveme každý monomorfizmus $\psi : M \to L$ taký, že platí $\psi(k) = k$ pre $\forall\, k \in K$.*

Nech $K \leq L$. Potom K-automorfizmus telesa L je každý K-monomorfizmus $L \to L$. Množina všetkých K-automorfizmov telesa L vzhľadom ku skladaniu zobrazení tvorí grupu.

Definícia 5.4. *Grupu všetkých K-automorfizmov telesa L nazývame Galoisova grupa a značíme* $\mathrm{Gal}(K, L)$.

Príklad 5.5. Nech $\mathbb{R} \leq \mathbb{R}(i) = \mathbb{C}$ a ψ je $\mathbb{R}$-automorfizmus telesa $\mathbb{C}$. Pre $\psi(i) = j$, platí $j^2 = (\psi(i))^2 = \psi(i^2) = \psi(-1) = -1$ a keďže jediné prvky v $\mathbb{C}$ s takouto vlastnosťou sú $j = i$ alebo $j = -i$, máme 2 kandidátov na $\mathbb{R}$-automorfizmus $\mathbb{C}$

$$\psi_1 : x + iy \mapsto x + iy$$

$$\psi_2 : x + iy \mapsto x - iy.$$

Kde ψ_1 je identita a teda určite ide o $\mathbb{R}$-automorfizmus $\mathbb{C}$ a nie je ťažké ukázať o ψ_2, že je to $\mathbb{R}$-automorfizmus $\mathbb{C}$ a preto je $\mathrm{Gal}(\mathbb{R}, \mathbb{C})$ cyklická grupa rádu 2.

Príklad 5.6. Nech $K \leq L \leq \mathbb{C}$ sú telesá, kde L je rozkladovým nadtelesom ireducibilného polynómu f nad telesom K. Podľa vety 4.6 je L normálnym rozšírením. Nech $\alpha_1, \ldots, \alpha_n$ sú rôzne korene polynómu f, potom $L = K(\alpha_1, \ldots, \alpha_n)$. Vezmime ľubovoľné $\psi \in \mathrm{Gal}(K, L)$, potom $\psi(\alpha_i) = \alpha_j$, pretože

$$\psi(f(\alpha_i)) = f(\psi(\alpha_i)) = 0.$$

Teda $\psi(\alpha_i)$ je koreňov polynómu f. Zobrazenie ψ môžeme reprezentovať permutáciou π, kde $\pi(i) = j$ (vyjadruje ako sa korene polynómu, pri danom K-automorfizme, zobrazujú na seba). Z toho je vidieť, že Galoisová grupa takéhoto rozšírenia je izomorfná s podgrupou grupy $\mathbb{S}_n$.

Nech $K \leq L$ je rozšírenie telies, Potom $\mathcal{F}$ bude značiť množinu všetkých medzitelies rozšírenia $K \leq L$, t. j. $\mathcal{F} = \{M\,;\ K \leq M \leq L\}$. Ďalej $\mathcal{G}$ bude značiť množinu všetkých podgrúp Galoisovej grupy $\mathrm{Gal}(K, L)$, t. j. $\mathcal{G} = \{H\,;\ H \leq \mathrm{Gal}(K, L)\}$. Zadefinujme si zobrazenia :

$$^* : \mathcal{F} \to \mathcal{G} \qquad \text{a} \qquad ^\dagger : \mathcal{G} \to \mathcal{F},$$

kde $M^* = \mathrm{Gal}(M, L)$ pre $M \in \mathcal{F}$ a $H^\dagger = \{x \in L;\ \alpha(x) = x \text{ pre } \forall \alpha \in H\}$ pre $H \in \mathcal{G}$. Nie je ťažké overiť, že $M \leq M^{*\dagger}$ a $H \leq H^{\dagger *}$.

Veta 5.7. *Nech $K \leq L$ je konečné rozšírenie telies a H je konečná podgrupa Galoisovej grupy $\mathrm{Gal}(K, L)$, potom $[H^\dagger : K] = [L : K]/|H|$.*

Dôkaz. Keďže $H^\dagger$ je podteleso L platí $[L : K] = [L : H^\dagger][H^\dagger : K]$ a podľa vety 5.2 máme $[L : H^\dagger] = [H]$. □

Dôkaz nasledujúcich 2 tvrdení sa dá nájsť napríklad v [4].

Tvrdenie 5.8. *Nech $K \leq L$ je konečné a normálne rozšírenie telesa K. Potom pre $p \in K[x]$, kde p je ireducibilný nad K a má korene α, β v L, existuje K-automorfizmus τ telesa L taký, že $\tau(\alpha) = \beta$.*

Tvrdenie 5.9. *Nech $L \leq K$ je konečné a normálne rozšírenie telesa K a $K \leq M \leq L$. Nech τ je K-monomorfizmus $M \to L$. Potom existuje K-automorfizmus $\sigma : L \to L$ taký, že $\sigma|_M = \tau$.*

Veta 5.10. *Pre konečné rozšírenie telies $K \leq L$ sú nasledujúce podmienky ekvivalentné:*

1. *$K \leq L$ je normálne.*
2. *Nech $K \leq L \leq M$ je konečné rozšírenie, potom každý K-monomorfizmus z $L \to M$ je K-automorfizmus telesa L.*

3. *Nech $K \leq L \leq N$ sú telesá, kde N je konečné normálne rozšírenie telesa K, potom pre každý K-monomorfizmus z $\psi : L \to N$ platí, že ψ je K-automorfizmus telesa L.*

Dôkaz. Dokážeme nasledujúce implikácie (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2). Ak $K \leq L \leq M$ a τ je K-monomorfizmus $L \to M$. Rozšírenie $K \leq L$ je konečné, teda algebraické rozšírenie. Nech $\alpha \in L$ a $p \in K[x]$ taký, že $p(\alpha) = 0$, potom $\tau(p(\alpha)) = p(\tau(\alpha)) = 0$ teda $\tau(\alpha)$ je koreň polynómu p. Z predpokladu je rozšírenie telies $K \leq L$ normálne, t. j. $\tau(\alpha) \in L$ a teda $\tau(L) \leq L$. A keďže τ je monomorfizmus na konečno rozmernom vektorovom priestore L nad K, je dimenzia $[\tau(L) : K] = [L : K]$ z čoho vyplýva, že $\tau(L) = L$.

(2) $\Rightarrow$ (3). Z tvrdenia 4.8 existuje N, normálny uzáver $K \leq L$, ktorý potrebné vlastnosti má.

(3) $\Rightarrow$ (1). Nech f je ireducibilný polynóm v telese K a $\alpha \in L$ je koreň polynómu f. Polynóm f sa v telese N rozkladá na lineárne činitele. Ak $\beta \in N$ je koreň f podľa tvrdenia 5.8 existuje K-automorfizmus γ telesa N taký, že $\gamma(\alpha) = \beta$. Podľa predpokladu je to aj K-automorfizmus L, teda $\beta = \gamma(\alpha) \in L$. Takže polynóm f sa rozkladá v L a podľa vety 4.6 je rozšírenie $K \leq L$ normálne. □

Veta 5.11. *Nech $K \leq L$ je konečné rozšírenie a $[L : K] = n$. Potom existuje presne n rôznych K-monomorfizmov $L \to N$, kde N je normálny uzáver rozšírenia $K \leq L$.*

Dôkaz. Budeme postupovať matematickou indukciou vzhľadom k n. Ak $n = = 1$, potom $L = K$ a existuje jediný K-monomorfizmus z $L \to N$ a to identita.

Predpokladáme, že pre $[L : K] < n$ existuje presne $[L : K]$ rôzných K-monomorfizmov $L \to N$.

Nech $[L : K] = n$ a $\alpha \in L \backslash K$ a nech $p \in K[x]$ je minimálny polynóm prvku α, potom

$$[K(\alpha) : K] = \deg(p) = r > 1.$$

Ireducibilný polynóm p nad $K \leq \mathbb{C}$ má podľa 4.12 rôzne korene. Jeden z jeho koreňov $\alpha \in N$, čo je normálne rozšírenie telesa K. To znamená, že polynóm p sa v N rozkladá na lineárne činitele a má rôzne korene: $\alpha_1, \ldots, \alpha_r \in N$.

$$\begin{aligned} [L : K] &= [L : K(\alpha)] \cdot [K(\alpha) : K] \\ n &= [L : K(\alpha)] \cdot r \end{aligned}$$

Z indukčného predpokladu máme pre $s = n/r$ rôznych $K(\alpha)$-monomorfiz-

mov $\rho_1, \ldots, \rho_s : L \to N$. Z tvrdenia 5.8 máme r rôznych K-automorfizmov $\tau_1, \ldots, \tau_r : N \to N$ a $\tau_i(\alpha) = \alpha_i$. Definujme zobrazenia :

$$\Phi_{ij} = \tau_i \rho_j \ , \text{ kde } \ i \in 1 \ldots r \ \text{ a } \ j = 1 \ldots s.$$

Teda máme $n = rs$ zobrazení z $L \to N$, o ktorých dokážeme, že sú rôzne.

Nech $\psi : L \to N$ je K-monomorfizmus. Pretože $\psi(p(\alpha)) = p(\psi(\alpha)) = 0$ je $\psi(\alpha)$ koreň polynómu p a teda existuje α_i, také že $\psi(\alpha) = \alpha_i$. Zadefinujme zobrazenie $\tau_i^{-1}\psi$. To je $K(\alpha)$-monomorfizmus $L \to N$. Z indukčného predpokladu existuje ρ_j také, že $\tau_i^{-1}\psi = \rho_j$. Z toho vyplýva, že $\psi = \tau_i\rho_j$. Teda z $\tau_i\rho_j = \psi_1 = \psi_2 = \tau_k\rho_l$ vyplýva, že $i = k$ a $j = l$. □

Dôsledok 5.12. *Ak $K \leq L$ je konečné a normálne rozšírenie, tak existuje presne $[L : K]$ rôznych K-automorfizmom telesa L.*

Dôkaz. Chceme dokázať rovnosť $|\mathrm{Gal}(K, L)| = [L : K]$.
Z vety 5.11 máme $[L : K]$ rôznych K-monomorfizmov $L \to N$, kde N je normálne rozšírenie K obsahujúce L. A z vety 5.10 (1. $\Leftrightarrow$ 2.) máme $[L : K]$ rôznych K-automorfizmov telesa L. □

Veta 5.13. *Nech $K \leq L$ je konečné a normálne rozšírenie telesa K. Potom $G^\dagger = K$, kde G značí Galoisovu grupu rozšírenia $K \leq L$.*

Dôkaz. Nech $[L : K] = n$. Z dôsledku 5.12 je $|G| = n$. Nech $K_0 = G^\dagger$. Z vety 5.2 máme $[L : K_0] = n$, z čoho vyplýva, že $K_0 = K$. □

Veta 5.14. *Nech $K \leq L \leq M$ a $K \leq M$ je konečné rozšírenie. Potom počet rôznych K-monomorfizmov $L \to M$ je najviac $[M : K]$.*

Dôkaz. Nech N je normálny uzáver rozšírenia $L \leq M$. Z tvrdenia 4.8 je $[K : N] < \infty$. Pričom každý K-monomorfizmus $L \to M$ je aj K-monomorfizmus $L \to N$. Podľa vety 5.11 existuje $[L : K]$ rôznych K-monomorfizmov $L \to N$. Teda K-monomorfizmov $L \to M$ je maximálne $[L : K]$. □

Veta 5.15. *Ak $K \leq L$ je konečné rozšírenie telesa K s Galoisovou grupou $G = \mathrm{Gal}(K, L)$ a teleso $K = G^\dagger$, potom $K \leq L$ je normálne rozšírenie. T. j. Ak $\mathrm{Gal}(K, L)^* = K$, potom $K \leq L$ je normálne rozšírenie.*

Dôkaz. Z vety 5.2 máme $[L : K] = |G|$. To znamená, že máme n rôznych K-automorfizmov $L \to L$, teda aj n rôznych K-monomorfizmov $L \to N$, kde $K \leq L \leq N$. Podľa predošlej vety 5.14 existuje najviac n rôznych K-monomorfizmov $L \to N$. A to znamená, že každý K-monomorfizmus $L \to N$ je K-automorfizmus L. Podľa vety 5.10 je $K \leq L$ normálne rozšírenie telesa K. □

Lema 5.16. *Nech $K \leq M \leq L$ sú telesá a nech τ je K-automorfizmus $L \to L$, potom $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Dôkaz. Nech $\gamma \in M^*$, $x_1 \in \tau(M)$, teda existuje $x \in M$ také, že $\tau(x) = x_1$. Z

$$(\tau\gamma\tau^{-1})(x_1) = \tau\gamma(x) = \tau(x) = x,$$

vyplýva, že $\tau M^* \tau^{-1} \leq \tau(M)^*$.
Nech je teraz $\rho \in \tau(M)^*$, potom

$$(\tau^{-1}\gamma\tau)(x) = \tau\gamma(x_1) = \tau(x_1) = x.$$

Z toho vyplýva, že $\tau(M)^* \leq \tau M^* \tau^{-1}$.

□

6 Základná veta Galoisovej teórie

V tejto kapitole prehľadne zhrnieme doteraz dokázané tvrdenia a vyslovíme niektoré z ich dôsledkov. Na záver uvedieme príklad, ktorý nám pomôže nasledujúcu vetu čo najlepšie pochopiť.

Na pripomenutie: Nech $K \leq L \leq \mathbb{C}$ a $G = \mathrm{Gal}(K, L)$, čo je grupa pozostávajúca zo všetkých K-automorfizmov telesa L. Ďalej nech $\mathcal{F}$ značí množinu všetkých telies M takých, že $K \leq M \leq L$ a $\mathcal{G}$ značí množinu všetkých podgrúp H grupy G. V predchádzajúcej kapitole sme definovali dve zobrazenia

$$\begin{aligned} {}^* : \mathcal{F} &\to \mathcal{G} \\ {}^\dagger : \mathcal{G} &\to \mathcal{F} \end{aligned}$$

a to tak, že pre $M \in \mathcal{F}$ je M^* grupou všetkých M-automorfizmov telesa L. Pre $H \in \mathcal{G}$ je $H^\dagger$ je maximálnym podtelesom L fixované grupou H.

Veta 6.1. *Nech $K \leq L$ je konečné a normálne rozšírenie v $\mathbb{C}$. Potom pre $G = \mathrm{Gal}(K, L)$ a $\mathcal{F}$, $\mathcal{G}$, *, † definované vyššie a M medziteleso $K \leq M \leq L$, platí:*

1. $|G| = [L : K]$.
2. *Zobrazenia * a † sú vzájomné inverzné.*
3. $[L : M] = |M^*| \quad a \quad [M : K] = |G|/|M^*|$.
4. *M je normálne rozšírenie telesa K práve vtedy, ak M^* je normálna podgrupa grupy G.*
5. $\mathrm{Gal}(K, M) \cong G/M^*$.

Dôkaz. Prvé tvrdenie je dôsledok 5.12. Rozšírenie $M \leq L$ je z vety 4.6 normálne rozšírenie. Z vety 5.13 je

$$M^{*\dagger} = M. \tag{6.1}$$

Nech $H \in \mathcal{G}$. Platí, že $H \leq H^{*\dagger}$ a z (6.1) je $H^{\dagger *\dagger} = (H^\dagger)^{*\dagger} = H^\dagger$. a z vety 5.2 dostávame $|H| = [L : H^\dagger] = [L : H^{\dagger *\dagger}]$ a $[L : H^{\dagger *\dagger}] = |H^{\dagger *}|$ z čoho plynie rovnosť $|H| = |H^{\dagger *}|$ a keďže sú to konečné grupy platí $H = H^{\dagger *}$. Čím sme dokázali druhé tvrdenie. Platnosť tretieho tvrdenia vyplýva z dôsledku 5.12.

Teraz dokážeme štvrté tvrdenie vety 6.1. Ak $K \leq M$ je normálne rozšírenie a $\tau \in G$, potom $\tau|_M$ je K-monomorfizmus $M \to L$ a podľa vety (5.10) je

to aj K-automorfizmus M. To znamená, že $\tau(M) = M$ a z lemy 5.16 máme $\tau M^* \tau^{-1} = M^*$. Preto M^* je normálna podgrupa grupy G.

Nech M^* je normálna podgrupa grupy G a τ nech je nejaký K-monomorfizmus $M \to L$. Podľa vety 5.9 existuje ψ K-automorfizmus $\psi : L \to L$ taký, že $\psi|_M = \tau$. Z lemy 5.16 máme $\psi(M)^* = M^*$. Podľa bodu (2) vety 6.1, máme $\psi(M) = M$, preto $\tau(M) = M$ a τ je K-automorfizmus M. Z vety 5.10 je $K \leq M$ normálne rozšírenie.

Nakoniec definujme zobrazenie

$$\begin{aligned} \Phi : G &\to \mathrm{Gal}(K, M) \\ \Phi(\tau) &= \tau|_M \qquad \tau \in G. \end{aligned}$$

Nie je sa tažké presvedčiť, že takto definované zobrazenie je grupový homomorfizmus, ktorý je surjektívny. A z vety o izomorfizme dostávame

$$\mathrm{Gal}(K, M) = \mathrm{Im}(\Phi) \cong G/\mathrm{Ker}(\Phi) = G/M^*.$$

Tým sme dokázali aj posledné tvrdenie vety 6.1. □

Dôležitosť tejto vety spočíva v existencii bijektívneho zobrazenia, nazývaného Galoisova korešpondencia, medzi podtelesami telesa L a podgrupami Galosiovej grupy telesa L. Týmto zobrazením sa prenášajú aj určité vlastnosti týchto matematických objektov.

Základnú vetu Galoisovej teórie ilustrujeme na nasledujúcom príklade.

Príklad 6.2. Uvažujme rozšírenie $\mathbb{Q} \leq K$, kde $K \leq \mathbb{C}$ je rozkladové nadteleso polynómu $f(x) = x^3 - 2$ nad $\mathbb{Q}$. Polynómu f môžeme v $\mathbb{C}$ rozložiť na lineárne činitele takto

$$f(x) = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}),$$

kde $\zeta_3^3 = 1$ a $\zeta_3 \neq 1$ (napr. $\zeta_3 = -1/2 + i(\sqrt{3}/2)$). Z toho vyplýva, že $K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Pre polynóm $f \in \mathbb{Q}[x]$ je teleso K rozkladovým nadtelesom, preto je rozšírenie $\mathbb{Q} \leq K$, podľa vety 4.6 normálne a konečné.

Pretože minimálny polynóm prvku $\sqrt[3]{2}$ nad $\mathbb{Q}$ je polynóm $x^3 - 2$ a minimálny polynóm prvku ζ_3 nad $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ je polynóm $x^2 + x + 1$. Platí

$$[K : \mathbb{Q}] = \left[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})\right] \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 6.$$

Podľa bodu 1 z vety 6.1 očakávaný počet prvkov grupy $\mathrm{Gal}(\mathbb{Q}, K)$ je 6. Označme korene polynómu f ako, $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta_3\sqrt[3]{2}$ a $\alpha_3 = \zeta_3^2\sqrt[3]{2}$. Každý $\mathbb{Q}$-automorfizmus telesa K je jednoznačne určený obrazom prvkov ζ_3 a α. A ich obraz musí byť koreňom príslušného ireducibilného polynómu nad $\mathbb{Q}$, čo znamená, že $\zeta_3 \mapsto \{\zeta_3, \zeta_3^2\}$ a $\alpha_1 \mapsto \{\alpha_1, \alpha_2, \alpha_3\}$. Nasledujúca tabuľka nám popisuje všetkých šesť $\mathbb{Q}$-automorfizmov telesa K.

Automorfizmus	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
Zobrazuje $\zeta_3 \mapsto$	ζ_3	ζ_3	ζ_3	ζ_3^2	ζ_3^2	ζ_3^2
Zobrazuje $\alpha_1 \mapsto$	α_1	α_2	α_3	α_1	α_2	α_3
Potom $\alpha_2 \mapsto$	α_2	α_3	α_1	α_3	α_1	α_2
Potom $\alpha_3 \mapsto$	α_3	α_1	α_2	α_2	α_3	α_1
Permutácia	1	(123)	(132)	(23)	(12)	(13)

Posledný riadok, stotožnuje daný $\mathbb{Q}$-automorizmus s permutáciou, ktorá označuje, ako sa pri danom $\mathbb{Q}$-automorfizme na seba zobrazujú korene α_1, α_2, α_3. Vidíme, že $\mathrm{Gal}(\mathbb{Q}, K)$ je izomorfná grupe $\mathbb{S}_3$ a jej podgrupy teda sú

$$\mathcal{G} = \{\mathbb{S}_3,\ \mathbb{A}_3,\ \{1,(12)\},\ \{1,(13)\},\ \{1,(23)\},\ 1\}\ .$$

Teraz spočítame prvky množiny $\mathcal{F}$. Na rozšírenie $\mathbb{Q} \leq K$ sa môžeme pozerať ako na vektorový priestor nad $\mathbb{Q}$, kde báza vektorového priestoru K je

$$\left\{1, \sqrt[3]{2}, \sqrt[3]{2^2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2^2}\zeta_3,\ \zeta_3\right\}.$$

Ľubovoľný prvok $x \in K$ sa dá vyjadriť ako

$$x = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2^2} + a_3\sqrt[3]{2}\zeta_3 + a_4\sqrt[3]{2^2}\zeta_3 + a_5\zeta_3\,,\ \text{ kde } a_i \in \mathbb{Q}.$$

Nech $\{\sigma_1, \sigma_6\}^* = M$. Teda M je maximálne teleso v $\mathbb{Q} \leq M \leq K$, ktoré je fixované zobrazením σ_1 a σ_6.

$$\begin{aligned}\sigma_6(x) &= a_0 + a_1\zeta_3^2\sqrt[3]{2} + a_2\zeta_3\sqrt[3]{2^2} + a_3\zeta_3\sqrt[3]{2} + a_4\sqrt[3]{2^2} + a_5\zeta_3^2 = \\ &= (a_0 - a_5) - a_1\sqrt[3]{2} + a_4\sqrt[3]{2^2} + (a_3 - a_1)\zeta_3\sqrt[3]{2} + a_2\zeta_3\sqrt[3]{2^2} - a_5\zeta_3\end{aligned}$$

Aby platilo $\sigma_6(x) = x$ musí byť $a_0 - a_5 = a_0$, $a_1 = -a_1$, atď. Z čoho dostávame $a_1 = a_5 = 0$ a $a_2 = a_4$ a preto

$$\begin{aligned}x &= a_0 + a_2\sqrt[3]{2^2} + a_3\sqrt[3]{2}\zeta_3 + a_2\sqrt[3]{2^2}\zeta_3 = \\ &= a_0 + a_2\sqrt[3]{2^2}(1 + \zeta_3) + a_3\sqrt[3]{2}\zeta_3 = \\ &= a_0 + a_3\sqrt[3]{2}\zeta_3 - a_2(\sqrt[3]{2}\zeta_3)^2.\end{aligned}$$

Keďže σ_1 je identita je $\{1,(13)\}^* = \mathbb{Q}(\zeta_3\sqrt[3]{2})$. Takto by sme postupovali so všetkými prvkami množiny $\mathcal{G}$. Výsledok je ilustrovaný na obrázku (Obr. 1), pod príkladom.

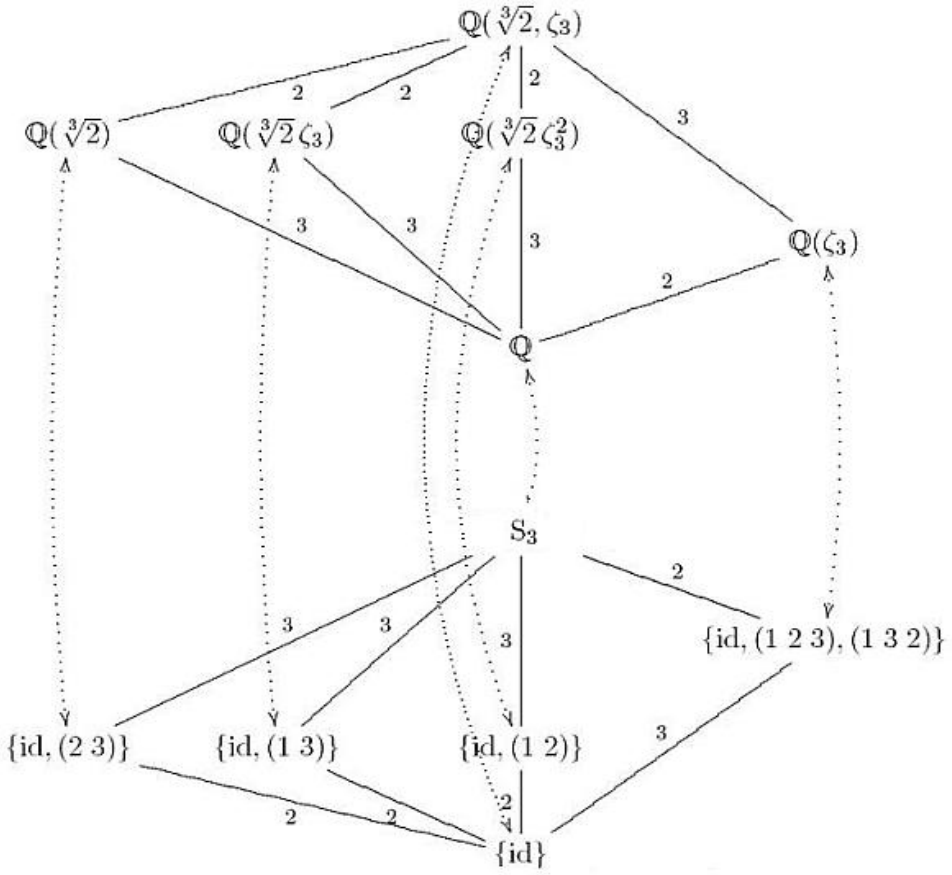
Podľa vety 6.1 je $\mathbb{Q} \leq M$ normálne rošírenie práve vtedy, ak M^* je normálna podgrupa grupy $G = \mathrm{Gal}(\mathbb{Q}, K)$. A naozaj – jediné normálne podgrupy grupy G sú $\mathbb{A}_3$ a 1. Teda M je buď teleso $\mathbb{Q}(\zeta_3)$, čo je normálne rozšírenie $\mathbb{Q}$, pretože pre polynóm x^2+x+1 je teleso $\mathbb{Q}(\zeta_3)$ rozkladovým nadtelesom. Alebo

$M = K$, čo je normálne rozšírenie. Ostatné telesa z $\mathcal{F}$ nie sú normálnym rozšírením telesa $\mathbb{Q}$, pretože v každom z nich leží aspoň jeden koreň polynómu $f(x) = x^3 - 2$, ale ani v jednom z nich neležia všetky korene polynómu f.

Počítajme $\mathrm{Gal}(\mathbb{Q}, \mathbb{Q}(\zeta_3))$. Každý $\mathbb{Q}$-automorfizmus telesa $\mathbb{Q}(\zeta_3)$ je jednoznačne určený obrazom prvku ζ_3 a obraz musí byť koreňom príslušného ireducibilného polynómu nad $\mathbb{Q}$, t. j. $\zeta_3 \mapsto \{\zeta_3, \zeta_3^2\}$. To nám dáva presne dva rôzne $\mathbb{Q}$-automorfizmy telesa $\mathbb{Q}(\zeta_3)$. Podľa vety 6.1 bodu 5, musí byť

$$\mathrm{Gal}(\mathbb{Q}, \mathbb{Q}(\zeta_3)) \cong \mathrm{Gal}(\mathbb{Q}, K)/\mathbb{A}_3,$$

čo naozaj platí, pretože $\mathrm{Gal}(\mathbb{Q}, K)/\mathbb{A}_3 \cong \mathbb{Z}_2$ a $\mathrm{Gal}(\mathbb{Q}, \mathbb{Q}(\zeta_3)) \cong \mathbb{Z}_2$.



Obr. 1: Galoisova korešpondencia pre rozšírenie $\mathbb{Q} \leq \mathbb{Q}(\zeta_3, \sqrt[3]{2})$.

7 Riešiteľné a jednoduché grupy

V tejto kapitole si povieme, čo rozumieme pod pojmom riešiteľné grupy a ukážeme si ich ich základné vlastnosti. V teórií riešiteľnosti rovníc pomocou radikálov zohrávajú tieto grupy veľmi dôležitú úlohu. Na záver dokážeme, že grupa permutácií $\mathbb{S}_n$, nie je pre $n \geqq 5$ riešiteľná.

Definícia 7.1. *Grupa G je riešiteľná, ak existuje konečná postupnosť jej podgrúp*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

spĺňajúca

1. $G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n$
2. G_{i+1}/G_i *je abelovská pre* $i = 0, \ldots, n-1$.

Príklad 7.2. Symetrická grupa $\mathbb{S}_4$ je riešiteľná, pretože existuje postupnosť jej podgrúp spĺňujúca obe podmienky definície 7.1

$$1 \ \triangleleft \ \mathbb{V} \ \triangleleft \ \mathbb{A}_4 \ \triangleleft \ \mathbb{S}_4,$$

kde $\mathbb{V}$ je Kleinova grupa $\mathbb{V} = \{1, (12)(34), (13)(24), (14)(23)\}$ a naozaj platí

$$\begin{array}{rcll} \mathbb{V}/1 & \cong & \mathbb{V} & \mathbb{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ je abelovská grupa,} \\ \mathbb{A}_4/\mathbb{V} & \cong & \mathbb{Z}_3 & \mathbb{Z}_3 \text{ je abelovská grupa,} \\ \mathbb{S}_4/\mathbb{A}_4 & \cong & \mathbb{Z}_2 & \mathbb{Z}_2 \text{ je abelovská grupa.} \end{array}$$

Každá abelovská grupa G je riešiteľná, lebo jej postupnosť $1 \triangleleft G$ vyhovuje podmienkam z definície.

Na pripomenutie uvádzam nasledujúce vety o izomorfizme grúp.

Veta 7.3 (2. veta o izomorfizme)**.** *Nech $K \leq H$ sú normálne podgrupy grupy G. Potom $H/K \triangleleft G/K$ a $(G/K)/(H/K) \cong G/H$.*

Veta 7.4 (3. veta o izomorfizme)**.** *Nech H, K sú podgrupy grupy G a nech $H \triangleleft G$. Potom $H \cap K \triangleleft K$ a $HK/H \cong K/(H \cap K)$.*

Veta 7.5. *Nech H je podgrupa grupy G a $N \triangleleft G$. Potom platí:*

1. *Ak je G riešiteľná, potom je H riešiteľná.*
2. *Ak je G riešiteľná, potom je G/N riešiteľná.*

3. Ak N a G/N sú riešiteľné, potom je G riešiteľná.

Dôkaz. 1. Nech

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

je postupnosť podgrúp G, kde G_{i+1}/G_i je abelovská grupa. Nech $H_i = G_i \cap H$, potom je $H_i \triangleleft H_{i+1}$ a

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i},$$

kde izomorfizmus dostávame použitím vety 7.4. Keďže G_{i+1}/G_i, je abelovská je aj jej podgrupa H_{i+1}/H_i abelovská a teda H je riešiteľná.

2. Nech G_i sú podgrupy grupy G ako v bode 1, potom G/N má postupnosť podrúp je

$$1 = NN/N \triangleleft G_1N/N \triangleleft \cdots \triangleleft GN/N = G/N$$

s faktorgrupou

$$\frac{G_{i+1}N/N}{G_iN/N},$$

kde podľa 3. vety o izomorfizme je izomorfná s

$$\frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i},$$

kde nakonci je faktorgrupa abelovskej grupy G_{i+1}/G_i, teda G/K je riešiteľná.

3. Z toho, že N a G/N sú riešiteľné máme tieto dve postupnosti

$$1 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N$$

$$N/N \triangleleft G_1/N \triangleleft \cdots \triangleleft G_s/N = G/N$$

s abelovskými faktorgrupami. Pre grupu G definujme postupnosť

$$1 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N = N/N \triangleleft G_1 \triangleleft \cdots \triangleleft G_s = G,$$

kde faktor grupy sú buď N_{i+1}/N_i, ktoré sú z predpokladu abelovské, alebo G_{i+1}/G_i, ktoré sú izomorfné s abelovskou grupou

$$G_{i+1}/G_i \cong (G_{i+1}/N)/(G_i/N).$$

Teda G je riešiteľná. □

Definícia 7.6. *Grupa G je jednoduchá práve vtedy, ak jej jediné normálne podgrupy sú 1 a G.*

Veta 7.7. *Riešiteľná grupa G je jednoduchá práve vtedy, ak G je cyklická grupa prvočíselného rádu.*

Dôkaz. Každá cyklická grupa $\mathbb{Z}_p$ pre prvočíslo p je jednoduchá, pretože jej jediné podgrupy sú 1 a $\mathbb{Z}_p$. Tieto podgrupy sú abelovské a teda aj riešiteľné.

Naopak ak G je riešiteľná grupa, máme z definície 7.1 postupnosť

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G,$$

kde G_{i+1}/G_i pre $i = 0, \ldots, n-1$ je abelovská faktorgrupa. Môžeme predpokladať, že $G_{i+1} \neq G_i$ a keďže G je jednoduchá, musí byť $G_{n-1} = 1$ a $G = G_n/G_{n-1}$. Teda G je abelovská grupa, v ktorej každá jej pogrupa je normálna podgrupa. Nech $1 \neq g \in G$, potom $H = \langle g \rangle = \{g^k; k \in \mathbb{Z}\}$ je podgrupa G a teda $H = G$. To znamená, že G je cyklická. Ak by G bola nekonečná grupa, platilo by, že $g \neq g^2$ a $g \notin \langle g^2 \rangle$. To by znamenalo, že $\langle g^2 \rangle$ je vlastná podgrupa G, takže G je konečná cyklická grupa rádu n. Grupa G má toľko podgrúp, koľko má deliteľov n, teda n musí byť nutne prvočíslo. □

Skôr než dokážeme vetu 7.9, pripomenieme si niektoré pojmy a tvrdenia o symetrických grupách.

Poznámka 7.8. *Nech $i_1, i_2, \ldots, i_k$ je postupnosť rôznych prvkov množiny $M = \{1, 2, \ldots, n\}$. Permutáciu $\alpha \in \mathbb{S}_n$ takú, že $\alpha(i_1) = i_2, \ldots, \alpha(i_{k-1}) = (i_k), \alpha(i_k) = i_1$ a $\alpha(i) = i$ pre $i \in M \backslash \{i_1, \ldots, i_k\}$, nazveme cyklom dĺžky k a budeme značiť $\alpha = (i_1 i_2 \ldots i_k)$. Cyklus dĺžky 2 nazveme transpozícia. Dva cykly α, β sú nezávislé, ak $\alpha \cap \beta = \emptyset$.*

Pre nezávislé cykly α, β platí $\alpha\beta = \beta\alpha$. Každú neidentickú permutáciu môžeme rozložiť na súčin nezávislých cyklov. Každú permutáciu môžeme rozložiť na súčin transpozíc, t. j. množina transpozíc $\{(1i);\ i = 2, \ldots, n\}$ je množina generátorov $\mathbb{S}_n$. Ak $n \geqq 3$ potom množina cyklov dĺžky tri tvaru $\{(12i);\ i = 3, \ldots, n\}$ je množina generátorov $\mathbb{A}_n$. Ak α je cyklus dĺžky k, potom α^k je identická permutácia.

Veta 7.9. *Pre $n \geqq 5$ je alternujúca grupa $\mathbb{A}_n$ jednoduchá.*

Dôkaz. Nech $1 \neq H \triangleleft \mathbb{A}_n$. Chceme dokázať, že potom je nutne $H = \mathbb{A}_n$. Na to nám bude podľa poznámky 7.8 stačiť dokázať, že H obsahuje všetky 3-cykly v tvare $(12x)$. Nech $1 \neq \alpha \in H$. Permutáciu α vyberieme z H tak, aby obsahovala čo najviac samodružných bodov. Nech $\alpha = \tau_1 \ldots \tau_r$ je rozklad na nezávislé cykly. Všetky cykly τ_i majú nutne rovnakú dĺžku. Ak by tomu tak nebolo, môžeme predpokladať, že τ_1 je cyklus s najkratšou dĺžkou k (násobenie nezávislých cyklov je komutatívne). Potom $\alpha^k = {\tau_1}^k \ldots {\tau_r}^k = {\tau_2}^k \ldots {\tau_r}^k$,

pretože ${\tau_1}^k$ je identická permutácia. To by znamenalo, že α^k má viac samodružných bodov a to je spor s výberom permutácie α.

Nech k označuje spoločnú dĺžku cyklov τ_i. Predpokladajme, že $k > 3$ a nech $\tau_1 = (i_1 \dots i_k)$ a $(i_1 i_2 i_k) \in \mathbb{A}_n$. Potom

$$\beta = \alpha(i_1 i_2 i_k)\alpha^{-1}(i_1 i_2 i_k)^{-1} \in H$$

a keďže násobenie nezávislých cyklov je komutatívne, dostávame

$$\beta = \tau_1(i_1 i_2 i_k)(i_1 i_2 i_k)^{-1}(i_1 i_2 i_k)^{-1} = (i_k i_3 i_1).$$

To znamená, že $\beta \neq 1$ má viacej pevných bodov ako α, čo je spor s voľbou α. Teda pre k musí platiť $k \leq 3$.

Ak by $k = 2$ a $r > 2$ a keďže α je párna permutácia, musí byť nutne $r \geqq 4$, teda

$$\alpha = (ab)(cd)(ef)(gh)\dots$$

a zvoľme $\tau = (ad)(be) \in \mathbb{A}_n$. Potom opäť dostaneme

$$\beta = \tau\alpha\tau^{-1}\alpha^{-1} = (ad)(be)(bc)(af) \in H$$

a pretože β zobrazuje $g \to g$ a $h \to h$ dostávame spor. (β má viac samodružných bodov ako α.)

Nech teraz $k = 2$, $r = 2$, $\alpha = (ab)(cd)$ a $\tau = (ae)(cd)$, pričom vďaka $n \geqq 5$ môžeme predpokladať, že a, b, c, d, e sú rôzne prvky a

$$\beta = \tau\alpha\tau^{-1}\alpha^{-1} = (aeb) \in H.$$

A opäť má β viacej samodružných bodov ako α a to je spor.

Nech $k = 3$, $r \geqq 2$, $\alpha = (abc)(def)\dots$ a $\tau = (ad)(be) \in \mathbb{A}_n$, potom

$$\beta = \tau\alpha\tau^{-1}\alpha^{-1} = (ad)(cf) \in H,$$

To opäť odporuje voľbe α. Ukázali sme, že H obsahuje 3-cyklus. Bez ujmy na všeobecnosti predpokladajme, že $(123) \in H$. Ostáva nám ukázať, že H obsahuje všetky 3-cykly tvaru $(12x)$. Zvolíme x a y tak aby $1, 2, 3, x, y$ boli rôzne, potom

$$(12x) = (3xy)(123)(3xy)^{-1} \in H$$

A podľa poznámky 7.8 je $H = \mathbb{A}_n$.

□

Dôsledok 7.10. *Pre $n \geqq 5$, symetrická grupa $\mathbb{S}_n$ nie je riešiteľná.*

Dôkaz. Ak by $\mathbb{S}_n$ bola riešiteľná, potom podľa vety 7.5 by bola aj $\mathbb{A}_n$ riešiteľná. Podľa vety 7.9 je $\mathbb{A}_n$ jednoduchá grupa. Podľa vety 7.7 je prvočíselného rádu, ale $|\mathbb{A}_n| = \frac{1}{2}(n!)$, čo pre $n \geqq 5$ nie je prvočíslo. Obdržali sme spor. □

Dôsledok 7.11. *Alternujúca grupa $\mathbb{A}_n$ je jedinou netriviálnou normálnou podgrupou permutačnej grupy $\mathbb{S}_n$ pre $n \geqq 5$.*

Dôkaz. Dá sa jednoducho ukázať, že netriviálna normálna podgrupa $\mathbb{A}_n$ obsahuje párnu permutáciu. Nech N je netriviálna normálna podgrupa grupy $\mathbb{S}_n$. Potom $N \cap \mathbb{A}_n$ je normálna podrupa grupy $\mathbb{A}_n$. Keďže N obsahuje párnu permutáciu, potom z vety 7.9 by $N \cap \mathbb{A}_n = \mathbb{A}_n$. Z toho dostávame, že $\mathbb{A}_n \leq N$, teda nutne $N = \mathbb{A}_n$. □

Dôsledok 7.12. *Alternujúca grupa $\mathbb{A}_n$ nemá netriviálnu normálnu podgrupu pre $n \geqq 5$*

Dôkaz. Dôkaz vety 7.9. □

Posledná veta, ktorú budeme potrebovať z teórie grúp, je Cauchyho veta. Je uvedená bez dôkazu, ktorý je možné nájsť v [4].

Veta 7.13 (Cauchy)**.** *Nech G je konečná grupa stupňa n. Ak prvočíslo p delí n, potom grupa G obsahuje prvok stupňa p.*

8 Radikálove rozšírenie

Cieľom tejto kapitoly je odvodiť pomocou Základnej vety Galoisovej teórie podmienku, kedy je polynóm riešiteľný pomocou radikálov.

Definícia 8.1. *Rozšírenie $K \leq L \leq \mathbb{C}$ nazývame radikálovým rozšírením, ak $L = K(\alpha_1, \ldots, \alpha_m)$, kde pre $\forall j = 1, \ldots, m$ existuje $n_j \in \mathbb{N}$ také, že*

$$\alpha_j{}^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1}).$$

Príklad 8.2. Rozšírenie telesa $\mathbb{Q} \leq \mathbb{Q}(\alpha, \beta, \gamma)$, kde $\alpha = \sqrt[3]{11}$, $\beta = \sqrt{3}$, $\gamma = \sqrt[5]{\frac{7+\sqrt{3}}{2}}$ je radikálové, pretože $\alpha^3 = 11 \in \mathbb{Q}$, $\beta^2 = 3 \in \mathbb{Q}(\alpha)$, $\gamma^5 = = \frac{7+\beta}{2} \in \mathbb{Q}(\alpha, \beta)$.

Tvrdenie 8.3. *Konečnú postupnosť z definície 8.1 môžeme upraviť (predĺžiť) tak, že všetky n_j budú prvočísla.*

Dôkaz. Ako dôkaz vety 3.4. □

Lema 8.4. *Nech $K \leq L \leq M$, kde $K \leq L$ je radikálové rozšírenie a M normálny uzáver rozšírenia $K \leq L$, potom $K \leq M$ je radikálové rozšírenie.*

Dôkaz. Nech $L = K(\alpha_1, \ldots, \alpha_m)$, kde $\alpha_j{}^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$. Nech polynóm $f_i \in K[x]$ značí minimálny polynóm prvku α_i. Potom z vety 4.6 je M rozkladovým nadtelesom polynómu $F = f_1 \ldots f_m$. Ďalej nech $F(\beta) = 0$, potom existuje $i = 1, \ldots, m$ také, že $f_i(\beta) = 0$. Z vety 5.9 existuje K-automorfizmus $\psi : M \to M$ taký, že $\psi(\beta) = \psi(\alpha_i)$, t. j. $K(\alpha_i) \cong K(\beta)$. Z toho, že $K(\alpha_i)$ je radikálové je aj, $K(\beta)$ radikálové, teda M je radikálové. □

Nasledujúce dve lemy ukážu postačujúcu podmienku, kedy je Galoisova grupa abelovská.

Lema 8.5. *Nech K je podteleso $\mathbb{C}$ a L je rozkladové nadteleso polynómu $t^p - 1$ nad K, kde p je prvočíslo. Potom Galoisova grupa $\mathrm{Gal}(K, L)$ je abelovská.*

Dôkaz. Derivácia polynómu $t^p - 1$ je pt^{p-1} a je vidieť, že žiaden polynóm stupňa väčšieho ako 1 nedelí $t^p - 1$ a zároveň pt^{p-1}. Z toho vyplýva, že polynóm $t^p - 1$ má len jednoduché korene v L. Tieto korene tvoria multiplikatívnu grupu G a keďže sú všetky rôzne, je $|G| = p$, teda grupa G je cyklická. Nech ε je generátor tejto grupy. Potom $L = K(\varepsilon)$, teda každý K-automorfizmus $\psi : L \to L$ je určený obrazom prvku ε. Pritom nutne $\psi(\varepsilon)$ je koreňom polynómu $t^p - 1$. Teda každý K-automorfizmus L je v tvare

$$\psi_j(\varepsilon) = \varepsilon^j \quad \text{kde } j = 0, \ldots, p-1.$$

Platí $\psi_i \psi_j = \varepsilon^{ij} = \varepsilon^{ji} = \psi_j \psi_i$, teda grupa $\mathrm{Gal}(K, L)$ je naozaj abelovská. □

Lema 8.6. *Nech polynóm t^p-1, kde p je prvočíslo, sa v telese K rozkladá na lineárne činitele. Nech $a \in K$ a teleso L je rozkladovým nadtelesom polynómu $t^p - a$ nad K. Potom* $\mathrm{Gal}(K, L)$ *je abelovská.*

Dôkaz. Nech $\alpha \in L$ je nejaký koreň polynómu t^p-a. všetky korene polynómu $t^p - a$ sú v tvare $\alpha\varepsilon^j$, kde $\varepsilon \neq 1$ je koreň polynómu $t^p - 1$. Preto $L = K(\alpha)$, a teda každý K-automorfizmus $\psi : L \to L$ je určený obrazom prvku α. Pritom nutne $\psi(\alpha)$ je koreňom polynómu $t^p - a$. Teda každý K-automorfizmus L je v tvare

$$\psi_j(\alpha) = \varepsilon^j\alpha \quad \text{kde } j \in 0, \ldots, p-1 \text{ a } \varepsilon^j \in K.$$

Tiež platí : $\psi_i\psi_j(\alpha) = \varepsilon^{ij}\alpha = \varepsilon^{ji}\alpha = \psi_j\psi_i(\alpha)$, teda grupa $\mathrm{Gal}(K, L)$ je naozaj abelovská. □

Lema 8.7. *Ak $K \leq L$ je normálne a radikálové rozšírenie, potom* $\mathrm{Gal}(K, L)$ *je riešiteľná grupa.*

Dôkaz. Nech $L = K(\alpha_1, \ldots, \alpha_n)$, kde ${\alpha_j}^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$. Z tvrdenia 8.3 môžeme predpokladať, že n_j sú prvočísla a označme $n_1 = p$. Dôkaz prevedieme pomocou matematickej indukcie podľa n.

Pre $n = 0$ je $L = K$ a $\mathrm{Gal}(K, L) = \{\mathrm{Id}\}$, čo je riešiteľná grupa.

Ak by $\alpha_1 \in K$, potom $L = K(\alpha_2, \ldots, \alpha_n)$ a z indukčného predpokladu vyplýva, že $\mathrm{Gal}(K, L)$ je riešiteľná grupa. Teda predpokladajme, že $\alpha_1 \notin K$. Nech $f \in K[x]$ je minimálny polynóm prvoku α_1. Z predpokladu, že $K \leq L$ je normálne rozšírenie má polynóm f všetky korene v L. Podľa lemy 4.12 má polynóm f len jednoduché korene. Keďže $\alpha_1 \notin K$ je $\deg(f) \geqq 2$. Nech β je koreň polynómu f rôzny od α. Pretože polynóm f delí polynóm $x^p - \alpha^p$ pre $\varepsilon = \alpha_1/\beta$ platí, že $\varepsilon^p = 1$ a $\varepsilon \neq 1$. Prvky $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1} \in L$ sú korene polynómu $t^p - 1$, t. j. polynóm $t^p - 1$ sa v L rozkladá na lineárne činitele.

Nech teleso M je rozkladovým nadtelesom pre polynóm t^p-1 nad K, teda $M = K(\varepsilon)$. Uvažujme reťazec podtelies $K \leq M \leq M(\alpha_1) \leq L$.

Keďže $t^p - 1$ sa rozkladá v M a $\alpha_1 \in K \leq M$, vidíme z dôkazu lemy 8.6, že $M(\alpha_1)$ je rozkladovým nadtelesom polynómu $t^p - {\alpha_1}^p$ nad M. Z vety 4.6 vyplýva, že rozšírenie $M \leq M(\alpha_1)$ je normálne a z lemy 8.6 je $\mathrm{Gal}(M, M(\alpha_1))$ abelovská grupa a teda aj riešiteľná. Použitím bodu 5 vety (6.1), dostávame

$$\mathrm{Gal}(M, M(\alpha_1)) \cong \frac{\mathrm{Gal}(M, L)}{\mathrm{Gal}(M(\alpha_1), L)}.$$

Pritom $L = M(\alpha_1)(\alpha_2, \ldots, \alpha_n)$, z čoho vidieť, že $M(\alpha_1) \leq L$ je normálne a radikálové rozšírenie a z indukčného predpokladu vyplýva, že $\mathrm{Gal}(M(\alpha_1), L)$ je riešiteľná grupa. Podľa bodu 3 vety 7.5 je $\mathrm{Gal}(M, L)$ riešiteľná grupa.

Keďže M je rozkladovým nadtelesom polynómu $t^p - 1$ nad K, je rozšírenie $K \leq M$ normálne. Z lemy 8.5 je grupa $\mathrm{Gal}(K, M)$ abelovská. A opäť z vety 6.1 dostávame

$$\mathrm{Gal}(K, M) \cong \frac{\mathrm{Gal}(K, L)}{\mathrm{Gal}(M, L)}.$$

Pritom $\mathrm{Gal}(K, M)$ je riešiteľná (ábelovská) a vieme, že aj grupa $\mathrm{Gal}(M, L)$ je riešiteľná a podľa vety 7.5 je nutne aj grupa $\mathrm{Gal}(K, L)$ riešiteľná.

□

Veta 8.8. *Nech $K \leq L \leq M$ sú telesá v $\mathbb{C}$ a rozšírenie $K \leq M$ je radikálové, potom je Galoisova grupa $\mathrm{Gal}(K, L)$ riešiteľná.*

Dôkaz. Nech $K_0 = (\mathrm{Gal}(K, L))^\dagger$ a N je normálny uzáver rozšírenia $K_0 \leq M$,

$$K \leq K_0 \leq L \leq M \leq N.$$

Keďže $K_0 \leq M$ je radikálové, je z lemy 8.4 aj rozšírenie $K_0 \leq N$ normálne a radikálové. Z vety 5.15 je rozšírenie $K_0 \leq L$ normálne. Podľa vety 6.1 bodu 3 dostávame

$$\mathrm{Gal}(K_0, L) \cong \frac{\mathrm{Gal}(K_0, N)}{\mathrm{Gal}(L, N)}.$$

Pritom z lemy 8.7 je grupa $\mathrm{Gal}(K_0, N)$ riešiteľná. A keďže $K_0 \leq L \leq N$, kde $K_0 \leq N$ je normálne rozšírenie a $K_0 \leq L$ je tiež normálne rozšírenie je podľa vety 6.1 $\mathrm{Gal}(L, N)$ normálnou podgrupou grupy $\mathrm{Gal}(K_0, N)$. Aplikáciou bodu 2 vety 7.5 je $\mathrm{Gal}(K_0, L)$ riešiteľná grupa.

Pretože $\mathrm{Gal}(K_0, L) = \mathrm{Gal}(K, L)$ je $\mathrm{Gal}(K, L)$ riešiteľná grupa. □

Definícia 8.9. *Nech f je polynóm nad $K \leq \mathbb{C}$ a nech U je jeho rozkladovým nadtelesom. Polynóm f je riešiteľný pomocou radikálov, práve keď existuje teleso M také, že $U \leq M$ a rozšírenie $K \leq M$ je radikálové. Galoisovou grupou polynómu f nazveme grupu* $\mathrm{Gal}(K, U)$.

Preformulovaním vety 8.8 dotávame nasledujúce tvrdenie.

Veta 8.10 (Galois)**.** *Nech f je polynóm nad telesom $K \leq \mathbb{C}$. Ak f je riešiteľný pomocou radikálov, potom je jeho Galoisova grupa riešiteľná.*

Vo vete 8.10 platí aj opačná implikácia, dôkaz nájdete napríklad v [1]. Aby sme dokázali, že existujú polynómy stupňa väčšieho ako 5, ktoré nie sú riešiteľné pomocou radikálov, stačí nám nájsť polynóm, ktorého Galoisova grupa nie je riešiteľná.

9 Neriešiteľný polynóm

V tejto kapitole dokážeme, že polynóm $x^5 - 6x + 3$ nie je riešiteľný pomocou radikálov.

Vetu „polynóm $x^5 - 6x + 3$ nie je riešiteľný pomocou radikálov“ môžeme preformulovať do vety „Galoisova grupa polynómu $x^5 - 6x + 3$ nie je riešiteľná“.

K tomu nám poslúži nasledujúca lema.

Lema 9.1. *Nech p je prvočíslo a f ireducibilný polynóm stupňa p nad telesom $\mathbb{Q}$. Ak algebraická rovnica $f = 0$ má presne dva korene v $\mathbb{C}\backslash\mathbb{R}$. Potom Galoisova grupa tohto polynómu je (izomorfná) $\mathbb{S}_p$.*

Dôkaz. Všetky korene algebraickej rovnice $f = 0$ ležia v $\mathbb{C}$. Teda ak, U značí rozkladové nadteleso polynómu f, platí $U \leq \mathbb{C}$. Nech G je Galoisova grupa polynómu f, t. j. $G = \mathrm{Gal}(\mathbb{Q}, U)$. Grupa G pozostáva z permutácií, ktoré permutujú (rôzne) korene polynómu f, teda $G \leq \mathbb{S}_p$. Nech α je koreň polynómu f, potom platí

$$[U : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][U : \mathbb{Q}(\alpha)] = \mathrm{p} \cdot [U : \mathbb{Q}(\alpha)].$$

Teda $[U : \mathbb{Q}]$ je deliteľné prvočíslom p. Z vety 6.1 bodu 1, vyplýva, že p delí $|G|$ a teda podľa Cauchyho vety 7.13, grupa G obsahuje prvok stupňa p. Jediný prvok Grupy G stupňa p je p-cyklus.

Nech $\alpha_1, \alpha_2 \in \mathbb{C}\backslash\mathbb{R}$ sú korene polynómu f nad $\mathbb{Q}$. Nutne musia byť α_1 a α_2 komplexne združené čísla. Potom zobrazenie ψ, ktoré α_1 zobrazí na α_2, je $\mathbb{R}$-automorfizmus $\mathbb{C}$, teda aj $\mathbb{Q}$-automorfizmus U, pričom ψ zobrazuje $p - 2$ reálnych koreňov na seba, t. j. grupa G obsahuje 2-cyklus.

Budeme predpokladať, ze G obsahuje 2-cyklus (12) a p-cyklus $(12 \dots p)$. Potom G obsahuje aj prvky

$$\begin{aligned} (12\dots p)^{-1}(12)(12\dots p) &= (23) \\ (12\dots p)^{-1}(23)(12\dots p) &= (34) \\ &\dots \end{aligned}$$

Ďalej G musí obsahovať prvky

$$(12)(23)(12) = (13), \quad (13)(34)(13) = (14), \quad \dots$$

to znamená, že G obsahuje prvky $(1j)$ kde $j = 2 \dots p$. Podľa poznámky 7.8 je $G = \mathbb{S}_p$. □

Na zistenie, či f je ireducibilný polynóm nad $\mathbb{Z}$ sa nám bude hodiť Eisensteinovo kritérium. Dôkaz je možné nájsť napríklad v [4].

Veta 9.2 (Eisensteinovo kritérium)**.** *Nech* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *je polynóm nad* $\mathbb{Z}$*. Ak existuje prvočíslo* p *také, že*

$$(1)\ p \nmid a_n\,, \qquad (2)\ p \mid a_i\ (i = 0, \ldots, n-1)\,, \qquad (3)\ p^2 \nmid a_0\,,$$

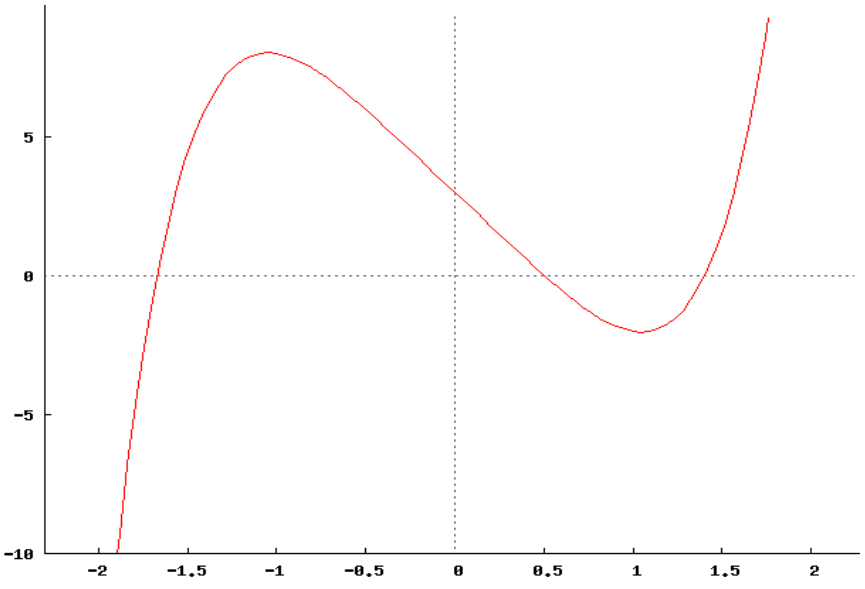
potom je f *ireducibilný nad* $\mathbb{Q}$*.*

Veta 9.3. *Polynóm* $x^5 - 6x + 3$ *nad* $\mathbb{Q}$ *nie je riešiteľný pomocou radikálov.*

Dôkaz. K dôkazu nám bude stačiť ukázať, že polynóm $x^5 - 6x + 3$ je ireducibilný nad $\mathbb{Q}$ a má presne tri reálne korene. Potom z lemy 9.1 je Galoisova grupa tohto polynómu rovná $\mathbb{S}_5$ a podľa vety 7.10 je grupa $\mathbb{S}_5$ neriešiteľná. Teda z vety 8.10 nie je polynóm $x^5 - 6x + 3$ riešiteľný pomocou radikálov.

Z Eisensteinovho kritéria dostávame ireducibilitu polynómu. Označme $f(x) = x^5 - 6x + 3$, potom $f(-2) = -17$, $f(0) = 3$, $f(1) = -2$ a $f(2) = 23$, keďže polynóm f je spojitá funkcia má polynóm f najmenej tri reálne korene.

Derivácia polynómu f, $D(f) = 5x^4 - 6$ ma dva reálne korene $x_1, x_2 \in \mathbb{R}$. Preto polynóm f na intervaloch $(-\infty, x_1)$ rastie(klesá), (x_1, x_2) klesá(rastie) (x_2, ∞) rastie(klesá). To znamená, že polynóm f má najviac tri reálne korene. Dokázali sme, že f ma presne tri reálne korene, teda nie je riešiteľný pomocou radikálov. □



Obr. 2: Graf funkcie $x^5 - 6x + 3$.

Literatúra

[1] Ian Stewart: *Galois theory - 3rd ed.*, Chapman & Hall/CRC mathematics.

[2] Harold M. Edwars: *Galois Theory*, Springer, New York, 1984.

[3] Lisl Gaal: *Classical Galois Theory*, American Mathematical Society, 1988.

[4] Ladislav Procházka a kol.: *Algebra*, Československá akadémia vied, Praha 1990.

[5] Jindřich Bečvář, Eduard Fuchs: *Matematika v proměnách věkú II*, Prometheus, Praha 2001.

Internet

http://www.maths.gla.ac.uk/∼ajb/dvi-ps/Galois.pdf

http://www.maths.bris.ac.uk/∼maarb/galois/notes.pdf

http://www.dpmms.cam.ac.uk/site2002/Teaching/II/Galois/Galois.pdf

http://www.maths.tcd.ie/∼dwilkins/Courses/311/311Galois.pdf